The Ultimate Guide to:

HARDENING WINDOWS SERVERS

THREATLOCKER

Introduction

Chapter 01 Run Patched Software

Chapter 02 Limit What Software can Execute

Chapter 03 Use Dual-Factor Authentication

Chapter 04 Block or Limit PowerShell

Chapter 05 Ringfence Applications

Chapter 06 Use as Little Software as Possible

Chapter 07 Use a Server Firewall

Chapter 08 Lock Down Folders per Application

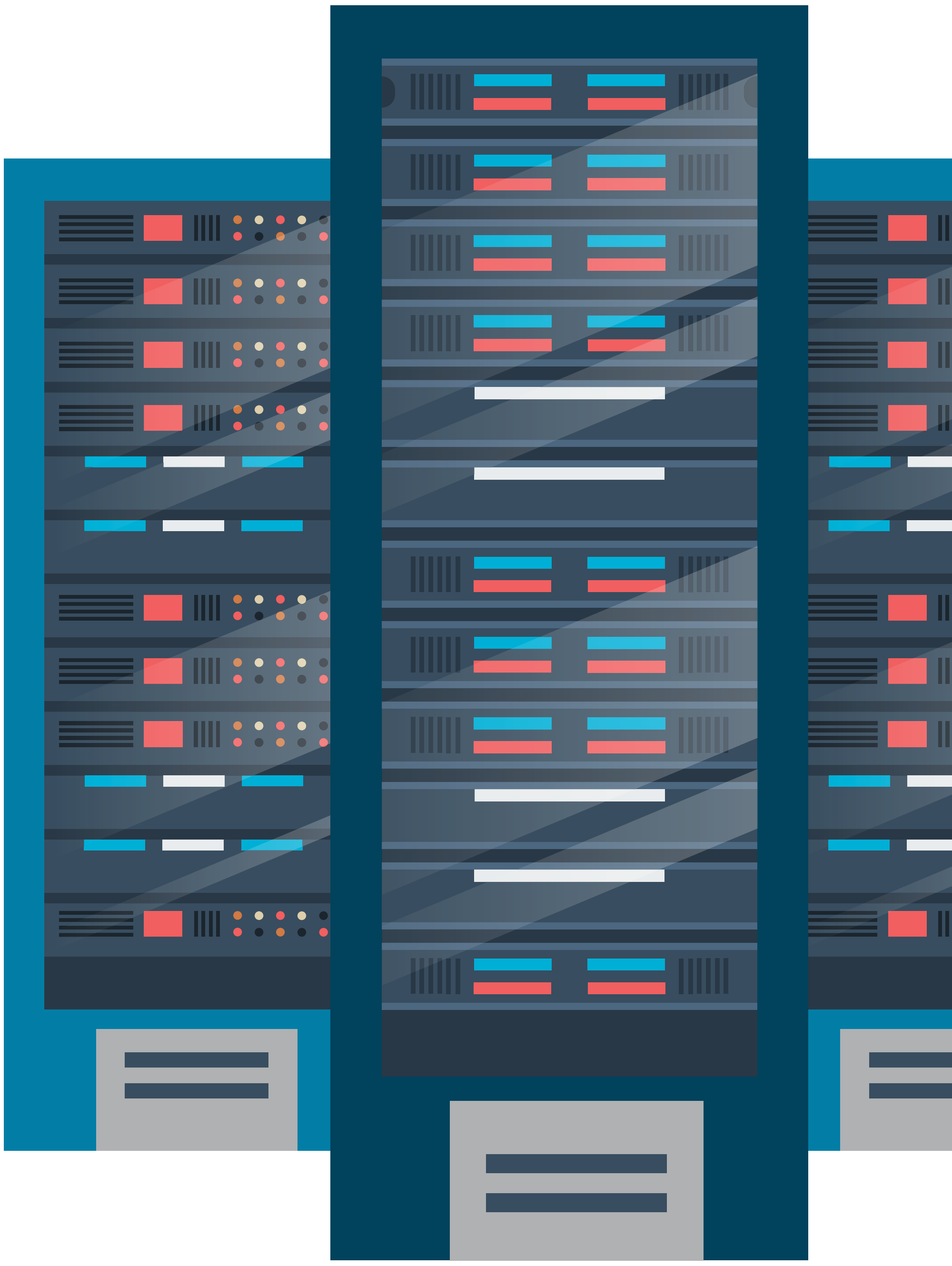
Chapter 09 Physically Secure Your Server or Use $Hidden Shares

Quick Tips!

Introduction

Microsoft Windows Servers have been the fundamental basis of small and large business networks since the early 2000s, and for many companies, servers are their lifeblood.

Servers are often the only entry point from the outside world. Workstations seldom require external ports to be open and most always use local firewalls to block inbound traffic. The nature of a server is to serve, and therefore, the Server Firewall is often disabled, or ports opened to allow necessary traffic. Whether you are running an in-house Exchange Server, Remote Desktop Server, File Server, Remote Management and Monitoring Server, or a Custom Application Server, you expose the server itself and your business to the risks of a vulnerability being exploited by attackers.



In 2017, EternalBlue, a computer exploit developed by the US National Security Agency (NSA), was leaked by the hacker group Shadow Brokers. Although Microsoft released a patch for the vulnerability, later that same year the WannaCry Ransomware used the exploit to infect unpatched machines and using servers to push malware to entire organizations. The EternalBlue vulnerability was in the Windows RPC stack, and while RPC is not likely to be an open port on the public network, it is a port that is open to enable file sharing. This allowed attackers to gain access to the server by infecting one workstation on the local network. The attackers gained access to a workstation through various sources including poor personal firewall management and a user opening a Microsoft Office document that contained malware.

Unfortunately, over the last five years, the EternalBlue exploit was not the only case where we have seen servers attacked. SolarWinds Orion, the Microsoft Exchange vulnerability, and Log4J are just a few other examples. IT and security professionals need to find ways to harden their servers without shutting down critical services. There is no silver bullet to stop a server from being compromised, but there are some steps you can take that will massively reduce the risk of your server being compromised.

At ThreatLocker our aim is to keep businesses safe and secure with our unique endpoint security solutions. We want to help you work smart and strengthen your security infrastructure from the ground up. Throughout this guide, you'll find top tips and best practices to help you better protect your business, learn more about the ThreatLocker solutions and how to harden your Windows Servers securely.

CHAPTER 01

Run Patched Software

As an IT Professional, you're always looking at ways to make your systems and environments more secure. One easy way to do this is to keep up with your patch management. Fixing the vulnerabilities that are susceptible to cyberattacks will help to significantly reduce security risks. Patching your systems and software also keeps everything up to date and running seamlessly, which will help you keep your systems supported and better protected at all times.

ThreatLocker currently analyzes data across 23,000 organizations. We analyze attacks against known vulnerabilities and investigate when these attacks attempted to execute. If we take the Exchange vulnerability as an example, we isolated the exploited file and queried previous like-kind exploits. Less than 7% of attacks happened before a patch was released for Microsoft Exchange, 30% of exploits occurred within one week of Microsoft releasing the patch, and the remaining software attack attempts happened over a week after there was a patch released.

It is difficult to patch servers immediately, as often you need to balance testing, the potential impact of the patch, and downtime. However, patch as fast as you can to reduce the likelihood of an exploit successfully infecting your server and systems.

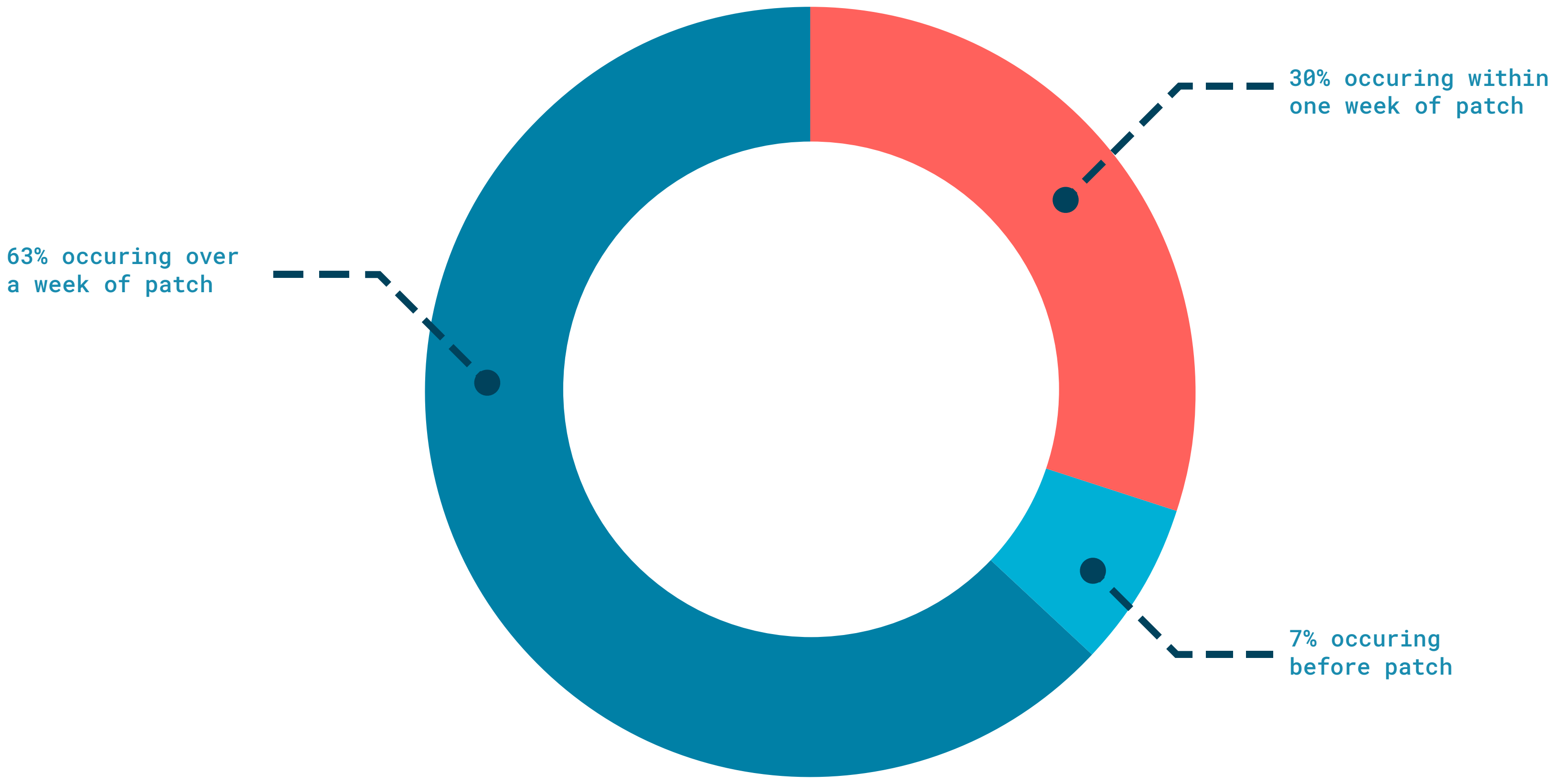


Figure 1. The above chart shows the data collected when analyzing the Exchange vulnerability.

Key Takeaway: If there is a patch this often means something is broken. Take note and act straight away. Patching is an essential step in better securing your servers.

CHAPTER 02

Limit What Software Can Execute

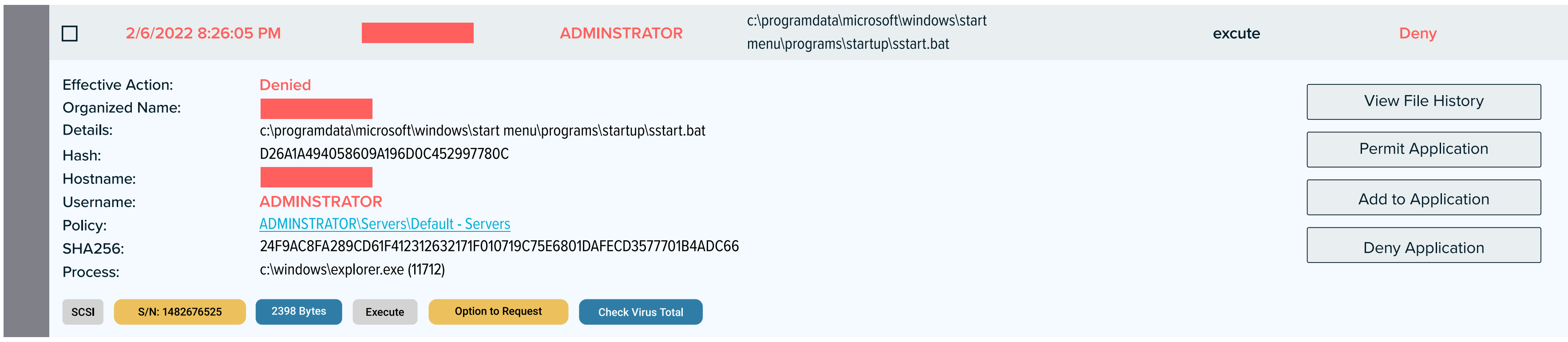
Application Allowlisting is a very effective method that helps to stop malicious software from running on your machine. In the case of both the EternalBlue and the Exchange exploit, the attacker executed software on the server using known vulnerabilities. In one case, it was an executable, and in the other, it was a batch file. The screenshot (*see Figure 2*) shows an attempted exploit of the Exchange vulnerability that was blocked by blocking a batch file from executing.

In addition to stopping malicious software from running, allowlisting makes it very difficult for an attacker to make use of good tools on your server if they do gain access. In most ransomware attacks, an attacker will use tools such as "Advanced IP. Scanner" to scan your network and locate your backup servers and other resources.

Utilizing allowlisting, you can stop unwanted software, including malware, from running on your servers and machines. You can also stop threat actors from making use of good software, enforce good behavior with your IT technicians, and stop bad behavior such as running a browser on your server.

When choosing an allowlisting solution, make sure that you pick a product that protects from DLLs, executables, and scripts. The solution should run at the kernel to block system-level executables. The built-in application allowlisting in Windows will not protect you from anything that runs from an exploit at the kernel.

Servers are generally easy to deploy allowlisting on because nothing should be changing dynamically by nature. ThreatLocker's advanced solution will automatically learn what is required to run in your environment and track updates so you do not have to manually permit each update, and it gives you an easy way to approve new software in 60 seconds.



□ 2/6/2022 8:26:05 PM [redacted] ADMINSTRATOR c:\programdata\microsoft\windows\start menu\programs\startup\sstart.bat excute Deny

Effective Action: Denied
Organized Name: [redacted]
Details: c:\programdata\microsoft\windows\start menu\programs\startup\sstart.bat
Hash: D26A1A494058609A196D0C452997780C
Hostname: [redacted]
Username: ADMINSTRATOR
Policy: ADMINSTRATOR\Servers\Default - Servers
SHA256: 24F9AC8FA289CD61F412312632171F010719C75E6801DAFECD3577701B4ADC66
Process: c:\windows\explorer.exe (11712)

Figure 2. An attempted exploit of the Exchange vulnerability that was blocked by blocking a batch file from executing.

Key Takeaway: By allowing only trusted files to run, you will immediately decrease the risk of a cyberattack. You can strengthen this process by implementing a Default Deny solution that will mitigate cyberattacks before they have the chance to infect your servers.

Book a Demo

CHAPTER 03

Use Dual-Factor Authentication

If an attacker gains access to your server, they can very easily navigate around your network and even bounce to other servers in your organization. Even in 2022, too many cyberattacks result from an attacker guessing a password on a customer's server, or phishing a password using malware on an administrator's PC.

Dual-Factor Authentication, otherwise known as 2FA, is a simple solution that requires a push to a mobile device or a one-time code before logging in. This solution can very easily stop an attacker from being able to log into your server. Installing 2FA should be standard on all shell access on all servers.

Key Takeaway: As an IT Professional, dual-factor authentication should be considered a standard security practice you implement. Most platforms are free, so it makes it easy to enable this extra layer of security across all applications.

CHAPTER 04

Block or Limit Powershell

PowerShell is one of the most powerful tools in the Windows Operating System, and *with great power comes great responsibility.* It is not likely that it will be completely possible to block PowerShell on your Windows as many applications may use it. However, you can check if PowerShell is being used on your server.

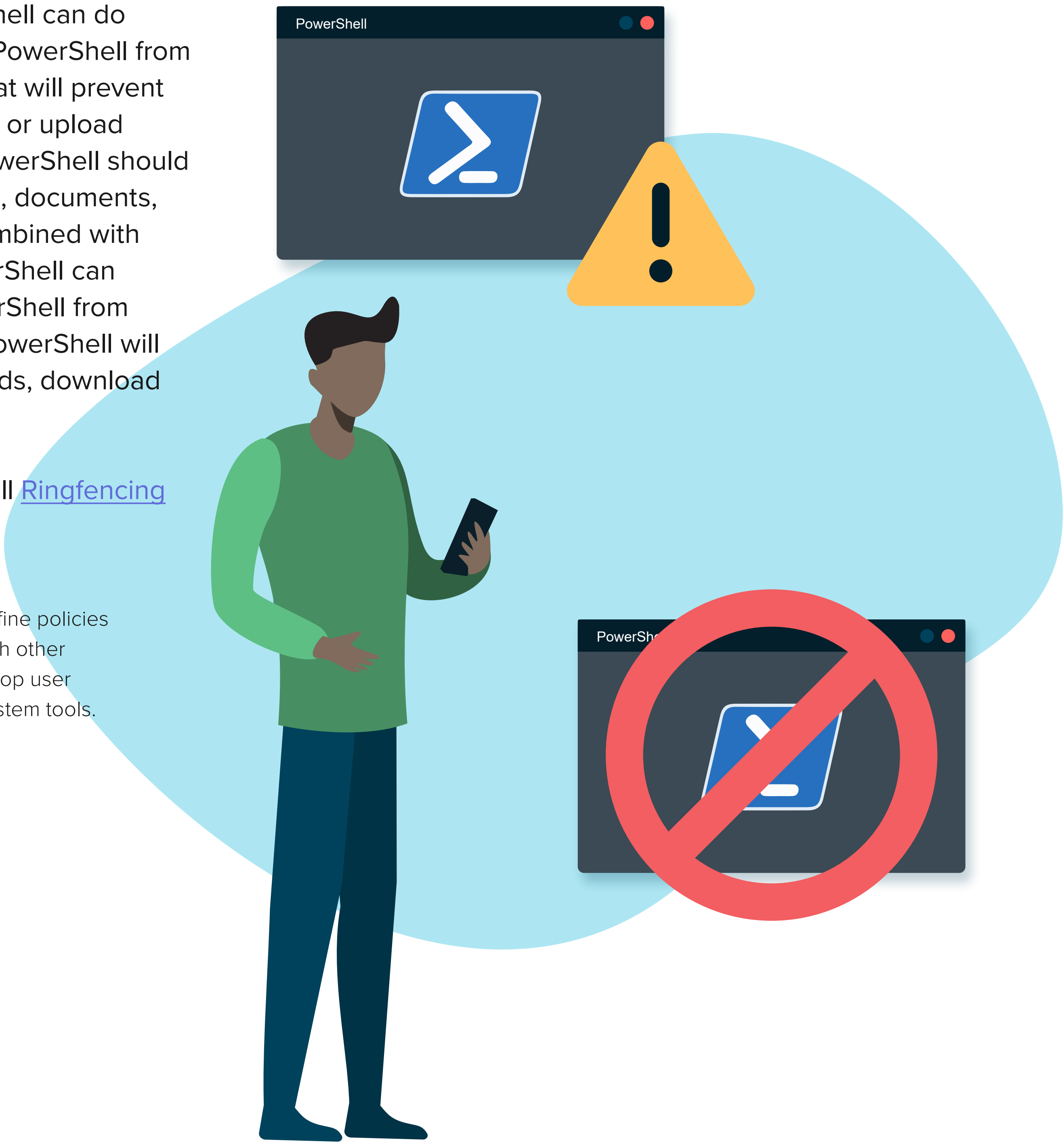
If you find PowerShell is being used in a limited way, e.g., for certain users or at certain times, create a policy to permit it for only those users or at those times.

You should also limit what PowerShell can do (i.e. Ringfence). For example, stop PowerShell from accessing documents and files. That will prevent it from being weaponized to delete or upload those files. Generally speaking, PowerShell should not need access to network shares, documents, or databases. Use Ringfencing, combined with storage control, to limit what PowerShell can access. You should also limit PowerShell from accessing the internet. This way, PowerShell will not be able to run remote commands, download files, or upload data.

ThreatLocker's standard PowerShell Ringfencing Policy is a good starting point.

Key Takeaway: Ringfencing allows you to define policies governing how an application can interact with other applications. Create Ringfencing policies to stop user frontend applications from interacting with system tools.

Book a Demo



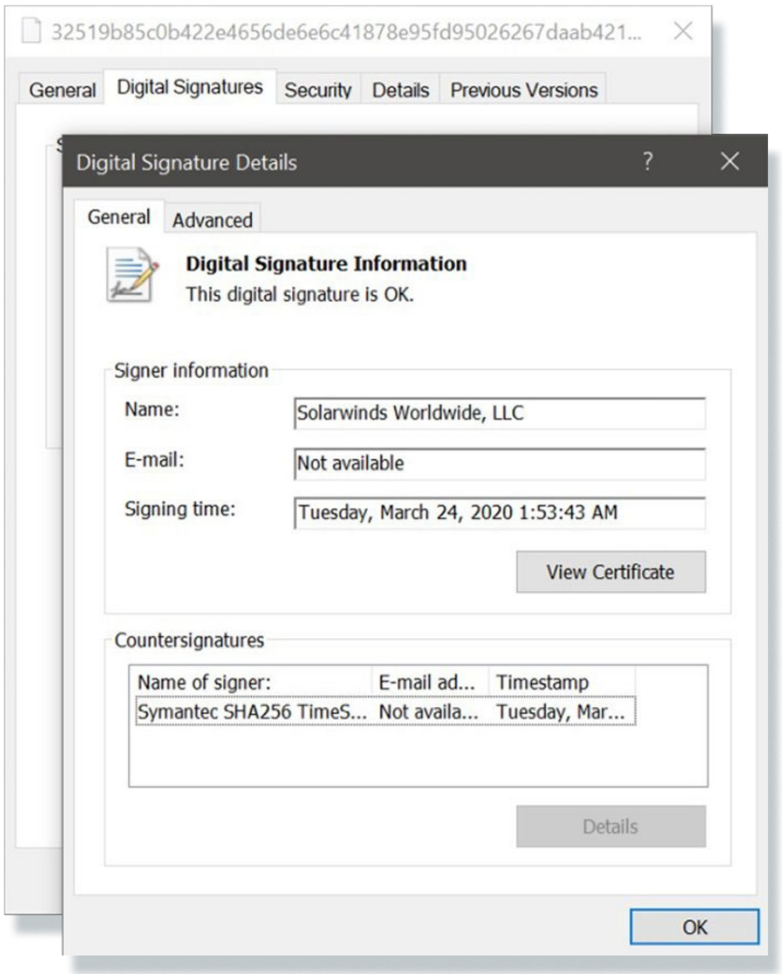
CHAPTER 05

Ringfence Applications

Every application you run on your server has access to all of the data on your server, and every other network share that any user logged into the server can access. In addition to accessing data, the application can also access the internet, access any other applications, and change the registry.

Any application can potentially be compromised through a vulnerability, misuse of a feature, or even a backdoor, whether intentionally or unintentionally planted. Patching and updating software will reduce your risks, but in many cases, the exploit happens before or immediately after the patch is issued.

The next level of protection is to limit what an application can do. You can prevent data exfiltration, or the application from getting malicious instructions, by stopping the application from going out to the internet, except for limited domains or I.P. addresses.



Digital Signature Information
This digital signature is OK.

Signer information

Name: Solarwinds Worldwide, LLC
E-mail: Not available
Signing time: Tuesday, March 24, 2020 1:53:43 AM

Countersignatures

Name of signer:	E-mail ad...	Timestamp
Symantec SHA256 TimeS...	Not availa...	Tuesday, Mar...

Figure 3. SolarWinds inadvertently delivering the backdoor malware as an update to the Orion software.

This is known as Ringfencing. Ringfencing allows for granular control over what applications are allowed to do. It enables you to limit interaction between applications, their access to files, the registry, and the internet. It helps to protect you against the weaponization of trusted applications whilst mitigating the risks posed by application vulnerabilities. In the case of SolarWinds Orion the hack, which saw 'SolarWinds inadvertently delivering the backdoor malware as an update to the Orion software' (see *Figure 3*), Ringfencing was able to foil an attack by preventing Orion from getting instructions. The damage is limited if you can take away an application's access to files that it does not need.

PowerShell, RegSRV, RunDLL, and many other Windows Components can be weaponized for malicious use. While it is not feasible to always block these applications, limiting which applications can call them will reduce the probability of said application launching an attack.

While you may not know the full capabilities of your applications, if you ringfence your applications in Monitor Only mode, you can review what they need over a learning period, and then lock them down after that period.

Key Takeaway: With ThreatLocker Ringfencing, you can configure an application's permissions in very granular detail. ThreatLocker has many templated applications, such as RunDLL, RegSRV, Zoom, Office, and PowerShell. In addition, you can also create your own policies.

Book a Demo

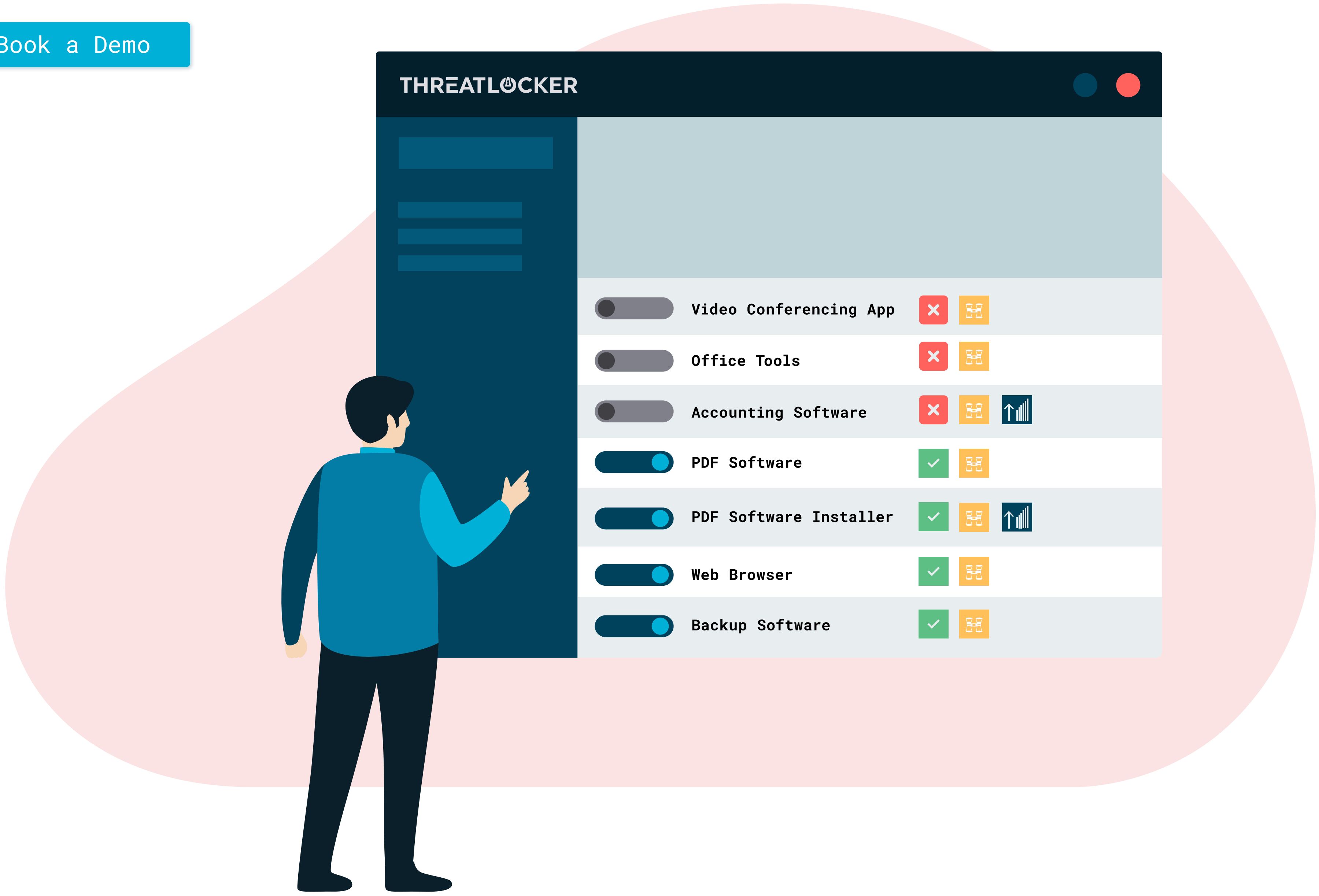
CHAPTER 06

Use as Little Software as Possible

It's no secret that the number of application vulnerabilities is increasing every year and we are struggling to stop them. The best way to minimize these attacks is to only use the software that is truly needed for work. Servers very rarely change and often do not require new applications to be installed, however, when they do they can open up the network to a litany of attacks. By using a minimal amount of applications across your server infrastructure, you can minimize the likelihood of these attacks. Rather than having multiple solutions on a system to give you system-specific information, use tools like BGInfo. BGInfo is a great tool to get a clear understanding of the resources and key information relating to the server you are working on.

Key Takeaway: Using as few pieces of software as possible, and allowing minimal to be installed on your machine is the best way to better protect your devices and your data. If you would like an easy way to manage the applications that are allowed to run on your machines, why not check out [ThreatLocker's Application Allowlisting](https://www.threatlocker.com).

Book a Demo



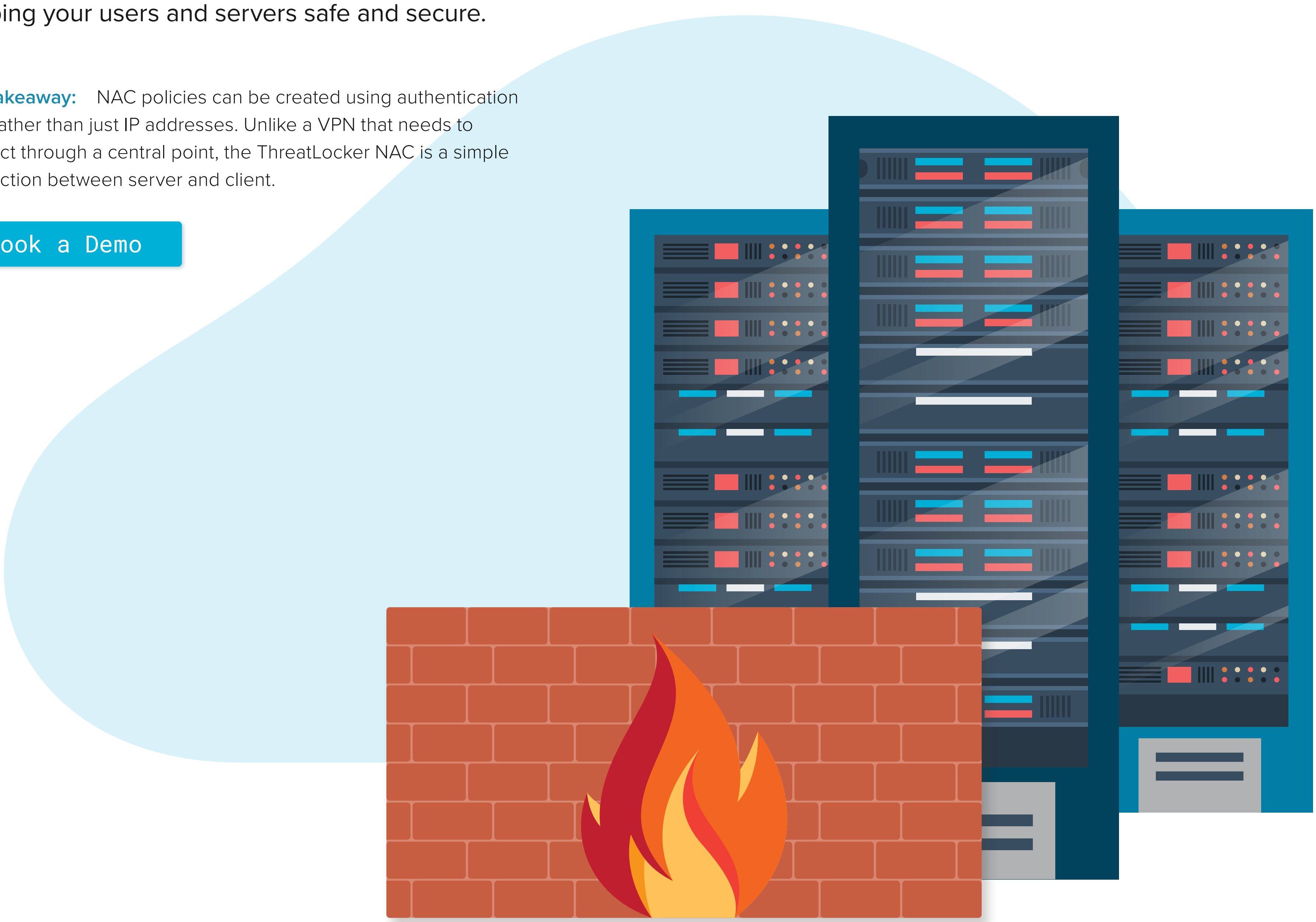
CHAPTER 07

Use a Server Firewall

With the increase in users working from home, traveling with work, and remote offices being set up, .the local network is now the internet and we are sharing this with threat actors, cyber gangs, and nation-state-sponsored hackers. The need to protect our remote workers and the way they connect to our local offices has never been more important. ThreatLocker's Network Access Control, NAC, allows IT Professionals to dynamically protect connections to devices based on IP addresses or even keywords. Rather than having an RDS gateway open on the web to anyone, you can now lock this down based on a specific keyword. If the gateway and the device running ThreatLocker both share the same keyword, the specific port will be opened and allow access. If they do not, the ThreatLocker Allowlisting approach will kick in, blocking access. Using tools such as NAC will enable you to better protect your network whilst keeping your users and servers safe and secure.

Key Takeaway: NAC policies can be created using authentication keys rather than just IP addresses. Unlike a VPN that needs to connect through a central point, the ThreatLocker NAC is a simple connection between server and client.

Book a Demo



CHAPTER 08

Lock Down Folders per Application

When an application is running on your machine, it has full access to everything that you have access to, including your files. A common action we see with ransomware is that it will initially scan for NFS, CIFS, and SMB shares, looking for places to infect. We need to lock down both our local folders and file stores, as well as our network locations. ThreatLocker's Storage Control enables you to easily lock down file and folder locations to individual applications such as Microsoft Office so that they are the only applications to access this data. ThreatLocker's Audit solution helps you to understand the applications that are accessing file and folder locations and then make educated decisions as to if they should continue to be allowed to access these locations. Using the ThreatLocker Storage Control solution, you can limit the access that ransomware and other nefarious applications have to your data.

Key Takeaway: Storage Control is an advanced storage solution that helps to protect data. It limits access to data by application, helping to protect against data exfiltration, and minimizing the damage caused by cyberattacks.

Book a Demo

CHAPTER 09

Physically Secure Your Server or Use $Hidden Shares

When sharing folders, use hidden shares. It makes it a little bit more difficult for attackers to document your network.

Hidden shares allow you to add another layer of protection for the data across your network. A network administrator should never assume that no one will ever be able to infiltrate the network; they should always assume that at some point a threat actor will gain access. It's best practice to put as many obstacles in the way to limit the damage that a threat actor can cause. This is where the importance of using hidden shares comes in. By adding a dollar sign to the end of a share name, you can prevent the resource from appearing when trying to access data through the network window. This simple step is incredibly powerful at making it harder for threat actors to access sensitive information.

Key Takeaway: Using hidden shares is a great way to protect and hide your data from threat actors. While this is only a step towards securing your data, it is a big step to take. If you would like to find more ways to secure your data, why not look at the ThreatLocker Storage Control Suite.

QUICK TIPS!

Block Outbound Server Access to the Internet

Servers are not laptops. Users should not need to browse the web from them. Most applications that run on servers do not need outbound access to the web. Even web services like Exchange or IIS do not need access to the web. The SolarWinds Orion data breach required the application to reach out to an attacker's server on AWS to get instructions. This is not uncommon, and blocking outbound web traffic is effective at foiling threats.

Review and Remove Old Accounts

A lot of cyberattacks make use of old unused accounts on your server. Review permitted logins on servers and remove them if they are not being used. Also, do not be afraid to remove accounts for current employees if they do not need them.

Restrict Login Times

Most cyberattacks happen during non-business hours. It allows attackers time to move around without being detected. Restrict login times by account. Some system admins might need to gain access 24/7, especially in a DR. situation, but many administrators only log in once a week to download a report. Limit their login times in Active Directory.

Set a Strong Password Policy

Set a group policy, either at the domain level for domain member servers or the local level for local servers, that requires at least ten characters, including a mixture of upper and lowercase letters, numbers, and special characters and educate your admins on good password examples. Then, ask your admins to attest in an affidavit that their password is secure and not reused anywhere else. Admins can lie in an affidavit as easily as in person, but in most cases, attesting to a formal document will encourage better behavior.

About ThreatLocker

ThreatLocker® is a global cybersecurity leader, providing enterprise-level cybersecurity tools to improve the security of servers and endpoints. ThreatLocker's combined Application Allowlisting , Ringfencing™, Storage Control and Privileged Access Management solutions are leading the cybersecurity market towards a more secure approach of blocking the exploits of unknown application vulnerabilities. To learn more about ThreatLocker visit: www.threatlocker.com

Book a Demo